PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-231595

(43)Date of publication of application : 22.08.2000

(51)Int.Cl. G06F 19/00
G06K 17/00
G07F 19/00
G07F 7/08

(21)Application number : 11-032793

(22)Date of filing : 10.02.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

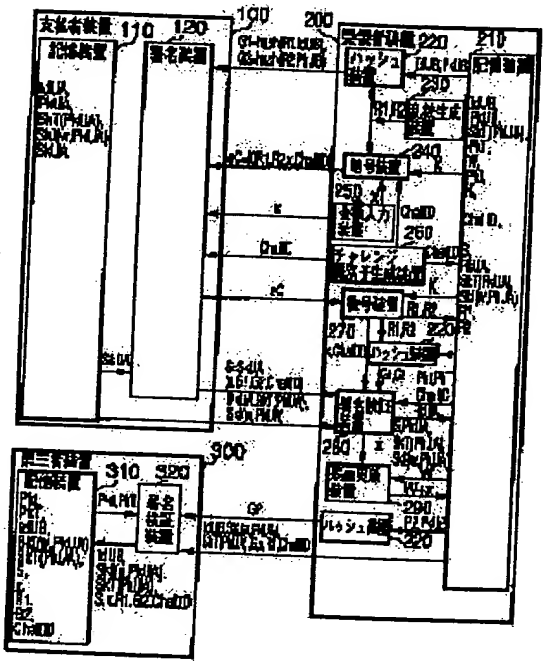
(72)Inventor : TORAMATSU KOICHI
MORIHATA HIDEMI

(54) METHOD AND DEVICE FOR TRANSFERRING IC CARD ELECTRONIC MONEY AND ITS PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To certify IC card balance to the third person when an IC card is damaged.

SOLUTION: A recipient calculates a random number R1, the hash value G1 of a recipient identifier IdUB, a random number R2 and the hash value G2 of a recipient public key, makes a value eC obtained by enciphering R1, R2, a received amount (x) and a challenge identifier ChallID with a key K, sends G1, G2, eC, (x), and ChallID to a payer, and the payer generates a signature S for reception information with a secret key and sends the recipient S, the signature SkT (PkUA) of an authentication institution of a payer public key PkUA and an issuing institution signature SkI (w and PkUA) of the amount (w). The recipient verifies them, when all of them are satisfied, then updates balance W into (x+ W) and sends a recipient public key PkUB, SkI (w and PkUA), SkT (PkUA), S, (x) and ChallID to the third person, and the third person performs signature verification of received information and stores the received information when they are accepted.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－231595
（P2000－231595A）
(43)公開日　平成12年８月22日(2000.8.22)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　15/30	３５０	３Ｅ０４０
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｒ	３Ｅ０４４
Ｇ０７Ｆ　19/00		Ｇ０６Ｆ　15/30	Ｊ	５Ｂ０５５
7/08			３６０	５Ｂ０５８
		Ｇ０７Ｄ　9/00	４７６	９Ａ００１

審査請求　未請求　請求項の数７　ＯＬ　（全６頁）　最終頁に続く

(21)出願番号　特願平11－32793

(22)出願日　平成11年２月10日(1999.2.10)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　虎松　恒一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　森畠　秀実
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

最終頁に続く

(54)【発明の名称】　ＩＣカード型電子マネー譲渡方法、その装置、そのプログラム記録媒体

(57)【要約】
【課題】　ＩＣカード破損時に、第三者にＩＣカード残高を証明可能とする。
【解決手段】　受領者は乱数Ｒ１、受領者識別子ＩｄＵＢのハッシュ値Ｇ１、乱数Ｒ２、受領者公開鍵のハッシュ値Ｇ２を求め、Ｒ１、Ｒ２、受領額ｘ、チャレンジ識別子ＣｈａｌｌＩＤを鍵Ｋで暗号化した値ｅＣを作り、Ｇ１、Ｇ２、ｅＣ、ｘ、ＣｈａｌｌＩＤを支払者へ送り、支払者はその秘密鍵で受領情報に対する署名Ｓを生成し、Ｓ、支払者公開鍵ＰｋＵＡの認証機関の署名ＳｋＴ（ＰｋＵＡ）、金額wの発行機関署名ＳｋＩ（ｗ，ＰｋＵＡ）を受領者へ送る。受領者はこれらを検証し、全て合格で、残高Ｗをｘ＋Ｗとし、支払者公開鍵ＰｋＵＢ、ＳｋＩ（ｗ，ＰｋＵＡ）、ＳｋＴ（ＰｋＵＡ）、Ｓ、ｘ、ＣｈａｌｌＩＤを第三者へ送り、第三者は受信情報の署名検証を行い、合格で受信情報を保存する。

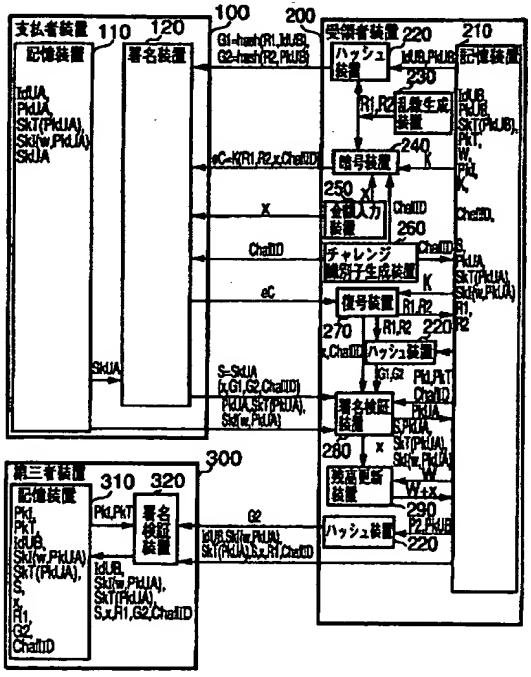


図　2

【特許請求の範囲】
【請求項１】　ＩＣカードで現金価値を管理する電子マネーを譲渡する方法において、
受領者装置が支払者装置から電子マネーを受領すると同時に、
第三者機関装置に譲渡に関する情報を送信し、
その第三者機関装置はその受信した譲渡に関する情報を記憶装置に保存することを特徴とする電子マネー譲渡方法。
【請求項２】　受領者装置から受信したチャレンジ情報に対し支払者装置が署名をして受領者装置へ送信し、受領者装置が受信した署名を検証することにより支払いが行われる電子マネー譲渡方法において、
受領者装置はチャレンジ情報を支払者装置に送信し、
支払者装置はチャレンジ情報に対する署名（以下、支払者署名）を作成し、
支払者署名を受領者装置に送信し、
受領者装置は支払者署名がチャレンジ情報に対して正しく署名されている事を検証し、
その検証に合格すると支払者署名を受領し、
第三者機関装置に支払者署名およびその署名検証に必要な情報を送信し、
第三者機関装置は支払者署名を保存することを特徴とする電子マネー譲渡方法。
【請求項３】　請求項２記載の方法において、
上記支払者署名がチャレンジ情報に対して正しく署名されている事を検証し、
検証に合格すると第三者機関装置にログ送信が可能であるかを問い合わせ、
可能であれば支払者署名を受領し、
その後第三者機関装置に支払者署名を送信することを特徴とする電子マネー譲渡方法。
【請求項４】　受領者装置から受信したチャレンジ情報に対し支払者装置が署名して受領者装置へ送り、受領者装置でその署名を検証することにより電子マネーによる支払いが行われる受領者装置であって、
受領者識別情報、支払者公開鍵などを記憶した記憶手段と、
チャレンジ情報を生成する手段と、
そのチャレンジ情報を支払者装置へ送信する送信手段と、
支払者装置から支払者署名を受信する受信手段と、
支払者署名を検証する署名検証手段と、
この検証に合格すると支払者署名を、上記記憶手段に記憶すると共に第三者機関装置へ送信する手段と、
を具備することを特徴とする受領者装置。
【請求項５】　上記検証に合格すると、第三者機関装置にログ送信が可能であるかを問い合わせる手段と、
ログ送信が可能である回答を受信すると、上記支払者署名の送信及び記憶手段への格納を行う手段と、
を具備する請求項４記載の受領者装置。
【請求項６】　受領者装置から受信したチャレンジ情報に対し支払者装置が署名して受領者装置へ送り、受領者装置でその署名を検証することにより電子マネーによる支払いが行われる受領者装置のコンピュータは、
チャレンジ情報を生成する処理と、
そのチャレンジ情報を支払者装置へ送信する処理と、
支払者装置から支払者署名を受信する処理と、
支払者署名を検証する処理と、
この検証に合格すると支払者署名を、記憶手段に記憶すると共に第三者機関装置へ送信する処理と、
を実行させるプログラムを記録した記録媒体。
【請求項７】　上記検証に合格すると、第三者機関装置にログ送信が可能であるかを問い合わせる処理と、
ログ送信が可能である回答を受信すると、上記支払者署名の送信及び記憶手段への格納を行う処理と、
を上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする請求項６記載の記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、電気通信システムやＩＣカードのような記録媒体を利用して電子マネーを譲渡する方法及びその装置に関する。
【０００２】
【従来の技術】電子マネーシステムはセンタ管理型と呼ばれるものとＩＣカード管理型と呼ばれるものの２つに大きく分類される。前者ではネットワーク上の管理センタにより利用者の所持する現金価値が管理されるが、トラフィックの集中を招くという問題点がある。
【０００３】一方ＩＣカード管理型は、ＩＣカード中に現金価値が存在するためトラフィックの問題が生じない。ＩＣカード型電子マネーでは、利用者ＩＣカードから商店サーバへの支払、利用者ＩＣカード間で行われる譲渡、共に２ノード間で情報をやりとりする事で行っていた。
【０００４】
【発明が解決しようとする課題】従来のＩＣカード型電子マネーの譲渡方法では、第三者が譲渡電子マネーの流通を管理できない、さらにはＩＣカード破損時にその残高を証明する事が出来ず、破損ＩＣカードに格納されていた電子マネー分の現金価値を利用者に保証できなくなるという問題点があった。
【０００５】上記問題はＩＣカード発行体と電子マネー発行体が一致する場合において顕著な問題となる。
【０００６】
【課題を解決するための手段】受領者装置が支払者装置からの電子マネーを受領後、第三者機関装置に支払者情報、受領者情報、金額情報を含むログを残す事で、第三者機関装置が譲渡電子マネーの流通を管理する事が可能

となる。さらに金融機関装置の情報とつきあわせれば、第三者機関装置が利用者のＩＣカード残高を管理する事が可能となる。

【０００７】「預入情報を解析する事で取引履歴が判明する方式」という制限はなく、広く一般の電子マネー方式に適用可能な手段である。又、受領者装置が電子マネーを受領する前に第三者機関装置に対してログ送信が可能か否かを問い合わせる事で、第三者機関装置が営業時間外であったなどの原因で、ログ送信が出来ない状態に陥る可能性を抑えられる。

【０００８】

【発明の実施の形態】この発明のシステム構成は図１に示すように支払者装置１００、受領者装置２００、第三者装置３００により構成される。

実施例１（図２参照）

支払開始前に予め、支払者は、正規の利用者である事を示す証として、支払者公開鍵ＰｋＵＡに対する認証機関の署名ＳｋＴ（ＰｋＵＡ）を入手し、電子マネーを所持している事を示す証として、金額w、および支払者公開鍵に対する電子マネー発行機関の署名ＳｋＩ（w，ＰｋＵＡ）、つまりＰｋＵＡに対する金額wの電子マネーを入手し、これらを支払者装置１００の記憶装置１１０に格納してある。

【０００９】受領者は、認証機関の公開鍵ＰｋＴおよび発行機関の公開鍵ＰｋＩを入手し、秘密鍵Ｋを作成して保持し、これらを受領者装置２００の記憶装置２１０に格納してある。支払い時に、受領者装置２００は、乱数生成装置２３０より乱数Ｒ１，Ｒ２を生成し、受領者ＩＤ（以下、ＩｄＵＢ）と乱数Ｒ１のハッシュした値Ｇ１、および受領者公開鍵（以下、ＰｋＵＢ）と乱数Ｒ２のハッシュした値Ｇ２、をそれぞれハッシュ装置２２０で計算し、チャレンジ識別子生成装置２６０より、時刻などチャレンジを識別する値（以下、ＣｈａｌｌＩＤ）を生成し、金額入力装置２５０より受領金額ｘを入力し、Ｒ１、Ｒ２、ｘ、ＣｈａｌｌＩＤを秘密鍵Ｋにより暗号装置２４０で暗号化した値ｅＣを求め、Ｇ１、Ｇ２、ｅＣ、ｘ、ＣｈａｌｌＩＤを支払者装置１００に送信する。

【００１０】支払者装置１００は、これらＧ１、Ｇ２、ｅＣ、ｘ、ＣｈａｌｌＩＤを受信すると、ｘ、Ｇ１、Ｇ２、ＣｈａｌｌＩＤに対する支払者署名Ｓを、支払者秘密鍵ＳｋＵＡを使って署名装置１２０で作成し、Ｓ、ｅＣ、支払者公開鍵ＰｋＵＡ、ＳｋＴ（ＰｋＵＡ）、ＳｋＩ（w、ＰｋＵＡ）を受領者装置２００に送信する。

【００１１】受領者装置２００はこれらを受信すると、ｅＣをＫにより復号装置２７０で復号化する事により、Ｒ１、Ｒ２、ｘ、ＣｈａｌｌＩＤを取出し、このＲ１、Ｒ２を用いてハッシュ装置２２０でＩｄＵＢとＲ１をハッシュしてＧ１を作成し、ＰｋＵＢとＲ２をハッシュしてＧ２を作成する。署名検証装置２８０で、これらハッシュ値Ｇ１、Ｇ２と復号したｘ、ＣｈａｌｌＩＤを用いてＳがｘ、Ｇ１、Ｇ２、ＣｈａｌｌＩＤに対する支払者署名になっている事をＰｋＵＡを使って確認し、ＳｋＴ（ＰｋＵＡ）が正しい署名である事を、ＰｋＴを使って検証し、ＳｋＩ（w，ＰｋＵＡ）が正しい署名である事を、ＰｋＩを使って検証し、全ての検証に合格した場合、保持していたＣｈａｌｌＩＤを消去し、つまり支払者からの金額ｘの受領で不要となった情報を消去し、支払者装置１００から受領したデータを保存し、残高更新装置２９０で残高をＷからＷ＋ｘへ更新し、Ｒ２、ＰｋＵＢのハッシュ値Ｇ２をハッシュ装置２２０で計算し、ＩｄＵＢ、ＳｋＩ（w，ＰｋＵＡ）、ＳｋＴ（ＰｋＵＡ）、Ｓ、ｘ、Ｒ１、Ｇ２、ＣｈａｌｌＩＤ、つまりＳとその署名・検証に必要な情報を第三者装置３００に送信する。この送信情報中のＩｄＵＢとＲ１はこれらによりＧ１を作ってＳの検証に用いることを可能としている。

【００１２】第三者装置３００は署名検証装置３２０で、ＳｋＴ（ＰｋＵＡ）が正しい署名である事を、ＰｋＴを使って検証し、ＳｋＩ（w，ＰｋＵＡ）が正しい署名である事を、ＰｋＩを使って検証し、全ての検証に合格した場合、ＩｄＵＢ、ＳｋＩ（w，ＰｋＵＡ）、ＳｋＴ（ＰｋＵＡ）、Ｓ、ｘ、Ｒ１、Ｇ２、ＣｈａｌｌＩＤをログとして記憶装置３１０に格納する。

【００１３】このように第三者装置３００には譲渡の経過を表わす情報が残されているから、電子マネー発行機関と第三者装置３００が協力すれば、どのＩＣカードにどれだけの残高があるかを、発行金額と譲渡金額とから知ることができる。なお１つのＩＣカードに対し、複数の電子マネーが発行されることがあるから発行機関の協力が必要である。

実施例２（図３参照）

支払開始前に予め、支払者は、正規の利用者である事を示す証として、支払者公開鍵ＰｋＵＡに対　する認証機関の署名ＳｋＴ（ＰｋＵＡ）を入手し、電子マネーを所持している事を示す証として、金額w、および支払者公開鍵ＰｋＵＡに対する電子マネー発行機関の署名ＳｋＩ（w，ＰｋＵＡ）を入手し、これらを記憶装置１１０に格納してある。

【００１４】受領者は、認証機関の公開鍵ＰｋＴおよび発行機関の公開鍵ＰｋＩを入手し、秘密鍵Ｋを作成して保持し、これらを記憶装置２１０に格納してある。支払い時に、受領者装置２００は乱数生成装置２３０より乱数Ｒ１，Ｒ２を生成し、受領者ＩＤ（以下、ＩｄＵＢ）と乱数Ｒ１のハッシュした値Ｇ１、および受領者公開鍵（以下、ＰｋＵＢ）と乱数Ｒ２のハッシュした値Ｇ２をそれぞれハッシュ装置２２０で計算し、チャレンジを識別する値（以下、ＣｈａｌｌＩＤ）をチャレンジ識別子生成装置２６０で生成し、受領金額ｘを金額入力装置２５０から入力し、Ｒ１、Ｒ２、ｘ、ＣｈａｌｌＩＤを秘

密鍵Kで暗号化した値eCを暗号装置240で生成し、これらG1、G2、eC、x、Chal1IDを支払者装置100に送信する。

【0015】支払者装置100は、G1、G2、eC、x、Chal1IDを受信すると、x、G1、G2、Chal1IDに対する支払者署名Sを署名装置120で支払者秘密鍵SkUAを使って作成し、S、eC、PkUA、SkT(PkUA)、SkI(w, PkUA)を受領者装置に送信し、受領者装置200は、これらを受信すると、eCをKにより復号装置270で復号化する事により、R1、R2、x、Chal1IDを取出し、このR1、R2を用いてハッシュ装置220でIdUBとR1をハッシュしてG1を作成し、PkUBとR2をハッシュしてG2を作成する。署名検証装置280で、これらハッシュ値G1、G2と復号されたx、Chal1IDを用いてSがx、G1、G2、Chal1IDに対する支払者署名になっている事を確認し、SkT(PkUA)が正しい署名である事を、PkTを使って検証し、SkI(w, PkUA)が正しい署名である事を、PkIを使って検証し、全ての検証に合格した場合、第三者装置300にログ送信が可能かどうかを問い合わせ装置280により問い合わせ、可能であるとの返答を第三者装置300のサービス状態返答装置340から得た場合、保持していたChal1IDを消去し、支払者装置100から受領したデータを保存し、残高をWからW+xへ残高更新装置290で更新し、IdUB、SkI(w, PkUA)、SkT(PkUA)、S、x、R1、G2、Chal1IDを第三者装置300に送信する。

【0016】第三者装置300は署名検証装置320でSkT(PkUA)が正しい署名である事を、PkTを使って検証し、SkI(w, PkUA)が正しい署名である事を、PkIを使って検証し、全ての検証に合格した場合、IdUB、SkI(w, PkUA)、SkT(PkUA)、S、x、R1、G2、Chal1IDをログとして記憶装置310に格納する。

【0017】上述において、R1、R2、x、Chal1IDをKで暗号化する代りに、R1、R2、x、Chal1IDをハッシュで撹乱して送信し、その返されたデータをR1、R2、x、Chal1IDで検証してもよい。あるいは受領者秘密鍵SkUBでR1、R2、x、Chal1IDを署名し、その返されたデータを署名検証してもよい。このようにチャレンジ情報(x、R1、R2、Chal1ID)を支払者装置で改ざんされないように処理して支払者装置へ送る場合は、Chal1IDのみを、支払者署名をもらうまで記憶しておけばその他のものは記憶しておく必要がなく、それだけ受領者装置の記憶装置として記憶容量が小さいものを使用できる。しかし、必ずしもそのようにすることなく、チャレンジ情報を受領者装置に、支払者署名をもらうまで保持すると共にチャレンジ情報をそのまま支払者装置へ送信してもよい。

【0018】

【発明の効果】従来のICカード型電子マネーの譲渡方法では、第三者が譲渡電子マネーの流通を管理したり、さらには破損ICカードに格納されていた電子マネー残高を確認し、利用者にその残高を保証したりする事が出来なかった。これに対し、この発明では、電子マネー譲渡に関する情報(支払者情報、受領者情報、金額情報)が第三者機関に残るため、金融機関の電子マネー発行情報とつきあわせれば、支払者、受領者の何れの利用者ICカードの残高を管理、保証する事が可能となった。譲渡ごとに第三者装置への通信分のトラフィック増加はあるが、この発明は商店への支払分のトラフィックには影響を与えないため、ICカード型のトラフィック軽減というメリットは継承している。

【0019】さらに受領者装置において、受領処理の前に第三者機関がサービス提供中であるかどうかを問い合わせる事によって、第三者機関が営業時間外などの理由でログ送信が不可能な状態に陥るのを抑える事が可能となった。

【図面の簡単な説明】

【図1】この発明の構成要素を示すブロック図。

【図2】この発明の実施例1の受領処理を示すブロック図。

【図3】この発明の実施例2の受領処理を示すブロック図。

【図1】

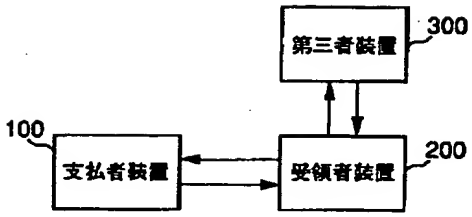

第三者装置
300
100
支払者装置
受領者装置
200

図 1

【図2】

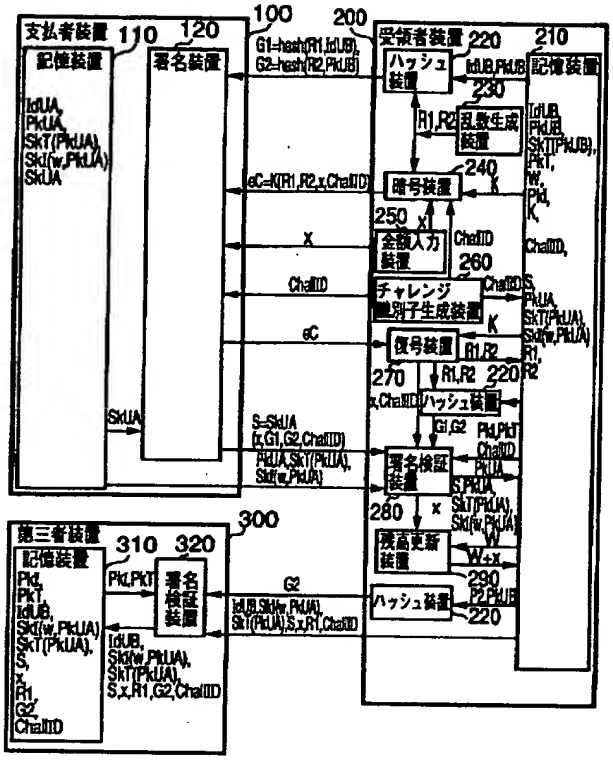

支払者装置
110
120
100
200
受領者装置
記憶装置
署名装置
ハッシュ装置
220
210
230
乱数生成装置
240
暗号装置
250
金額入力装置
260
チャレンジ識別子生成装置
270
復号装置
署名検証装置
280
残高更新装置
290
第三者装置
300
310
320

図 2

【図3】

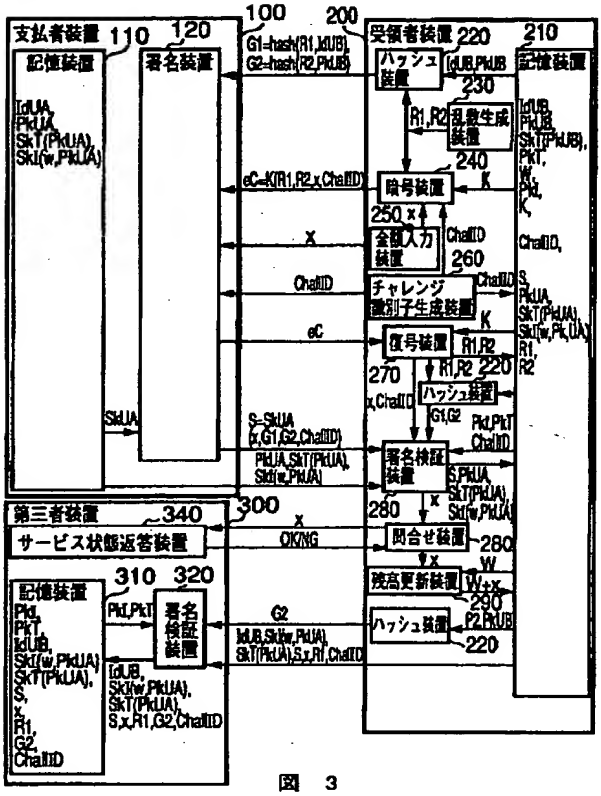


図 3

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
		G07F 7/08	J

Fターム(参考) 3E040 AA03 CA12 DA02
3E044 BA04 CA06
5B055 CB08 CB09 CC16 EE29 HA12
KK05 KK16
5B058 KA35 KA40 YA20
9A001 BZ03 EE03 JJ66 JJ67 LL03